IN THE CLAIMS

This listing of claims replaces all prior listings:

1. (currently amended) A computing environment, comprising:

an operating system;

a virtual machine operating on said operating system;

a first application operating on said virtual machine;

a second application operating on said virtual machine; ~~and~~

a first firewall control block, wherein said first firewall control block defines access privileges of said first application with respect to said second application, and further defines the access privileges of said second application with respect to said first application[[,]]; and

a second firewall control block, wherein said second firewall control block defines access privileges of said second application with respect to said first application, and further defines the access privileges of said first application with respect to said second application,

wherein said first firewall control block and the second firewall control block each includes a firewall control value and a firewall control indicator, the firewall control value including an application identifier data having a resource identifier and a proprietary identifier extension, the firewall control indicator being an indicator value represented by one or more bytes that indicate how the firewall control value should be interpreted with respect to access privileges of other applications, and

wherein when said firewall control indicator of said first firewall control block has a first indicator value, said first firewall control block compares said ~~first application's~~ proprietary identifier extension of said first firewall control block to said ~~second application's~~ proprietary identifier extension of said second firewall control block, and when said firewall control indicator of said first firewall control block has a second indicator value, said first firewall control block compares said ~~first application's~~ proprietary identifier extension and resource identifier of said first firewall control block to said ~~second application's~~ proprietary identifier extension and resource identifier of said second firewall control block.

2. (canceled)

3. (original) A computing environment as recited in claim 1, wherein said first firewall control block defines access privileges of said first application with respect to any other application in said computing environment, and further defines the access privileges of said any other application with respect to said first application.

4-5. (canceled).

6. (previously presented) A computing environment as recited in claim 1,
wherein said computing environment is a Java™ compliant computing environment, and
wherein said first and second applications are Java™ compliant applets.

7. (canceled).

8. (previously presented) A computing environment as recited in claim 1, wherein said computing environment is a Java™ card compliant computing environment, and,
wherein said first firewall control block is implemented as in the run rime environment.

9. (currently amended) A mobile computing device, comprising:
an operating system;
a Java™ compliant virtual machine operating on said operating system;
a first Java™ compliant applet operating on said Java™ compliant virtual machine;
at least one other Java™ compliant applet operating on said Java™ compliant virtual machine; and
a first firewall control block, wherein said first firewall control block defines access privileges of said first Java™ compliant applet with respect to the at least one other Java™ compliant applet operating on said Java™ compliant virtual machine, and further defines the access privileges of said at least one other Java™ compliant applet ~~Java™ compliant applet~~ with respect to said first Java™ compliant applet[[,]]; and
a second firewall control block, wherein said second firewall control block defines access privileges of said at least one other Java™ compliant applet with respect to the first Java™

compliant applet operating on said Java™ compliant virtual machine, and further defines the access privileges of said first Java™ compliant applet with respect to said at least one other Java™ compliant applet,

wherein said first firewall control block and said second firewall control block each includes a firewall control value and a firewall control indicator, the firewall control value including an application identifier data having a resource identifier and a proprietary identifier extension, the firewall control indicator being an indicator value represented by one or more bytes that indicate how the firewall control value should be interpreted with respect to access privileges of other Java™ compliant applets ~~applet~~, and

wherein when said firewall control indicator of said first firewall control block has a first indicator value, said first firewall control block compares said ~~first Java™ compliant applet's~~ proprietary identifier extension of said first firewall control block to said ~~at least one other Java™ compliant applet's~~ proprietary identifier extension of said second firewall control block, and when said firewall control indicator has a second indicator value, said first firewall control block compares said ~~first Java™ compliant applet's~~ proprietary identifier extension and resource identifier of said first firewall control block to said ~~at least one other Java™ compliant applet's~~ proprietary identifier extension and resource identifier of said second firewall control block.

10. (original) A mobile computing device as recited in claim 9, wherein said mobile device is a Java™ compliant smart card.

11-14. (canceled).

15. (previously presented) A mobile computing device as recited in claim 10, wherein for a firewall control block is defined for every Java™ compliant applet.

16. (currently amended) A method of providing security for a Java™ compliant computing environment that includes a Java™ virtual machine and a plurality of Java™ compliant applets that operate on said Java™ virtual machine, said method comprising:

receiving a request from a first Java™ compliant applet operating on a Java™ virtual machine to access a second Java™ compliant applet, the first Java™ compliant applet having a first firewall control block associated with it and the second Java™ compliant applet having a second firewall control block associated with it;

reading [[a]] the second firewall control block associated with said second Java™ compliant applet, said first firewall control block and said second firewall control block each including a firewall control value and a firewall control indicator, the firewall control value including an application identifier data having a resource identifier and a proprietary identifier extension, the firewall control indicator being an indicator value represented by one or more bytes that indicate how the firewall control value should be interpreted with respect to access privileges of the respective first or second Java™ compliant applet;

determining, based on said second firewall control block, whether said first Java™ compliant applet should be allowed to access said second Java™ compliant applet by determining whether said firewall control value of said second firewall control block has a first indicator value or a second indicator value, wherein

when said firewall control indicator of said second firewall control block has a first indicator value, said second firewall control block compares said ~~first Java™ compliant applet's~~ proprietary identifier extension of said first firewall control block to said ~~second Java™ compliant applet's~~ proprietary identifier extension of said second firewall control block, and

when said firewall control indicator of said second firewall control block has a second indicator value, said second firewall control block compares said ~~first Java™ compliant applet's~~ proprietary identifier extension and resource identifier of said first firewall control block to said ~~second Java™ compliant applet's~~ proprietary identifier extension and resource identifier of said second firewall control block; and

allowing said first Java™ compliant applet to access said second Java™ compliant applet when said determining determines that access should be allowed.

17. (currently amended) A method as recited in claim 16, wherein said method further comprises:

providing a reference to said first Java™ compliant applet with a reference to said second Java™ compliant applet when said determining determines that access should be allowed.

18. (currently amended) A method as recited in claim 16, wherein said providing of a reference comprises:

invoking a first method ~~implemented~~ that is implemented as a part of a Java™ management environment or Java™ system environment; and

invoking a second method that is implemented as a Applet class, as a result of said invoking of the second method.

19-21. (canceled).

22. (currently amended) A computer readable media including computer program code for providing security for a computing environment, said computer readable media comprising:

computer program code for receiving a request from a first application to access a second application, the first application having a first firewall control block associated with it and the second application having a second firewall control block associated with it;

computer program code for reading [[a]] the second firewall control block associated with said second application, said first firewall control block and said second firewall control block each including a firewall control value and a firewall control indicator, the firewall control value including an application identifier data having a resource identifier and a proprietary identifier extension, the firewall control indicator being an indicator value represented by one or more bytes that indicate how the firewall control value should be interpreted with respect to access privileges of the respective first or second application;

determining, based on said second firewall control block, whether said first application should be allowed to access said second application by determining whether said firewall control value of said second firewall control block has a first indicator value or a second indicator value, wherein

when said firewall control indicator of said second firewall control block has a first indicator value, said second firewall control block compares said ~~first application's~~ proprietary

identifier extension of said first firewall control block to said ~~second application's~~ proprietary identifier extension of said second firewall control block, and

when said firewall control indicator of said second firewall control block has a second indicator value, said second firewall control block compares said ~~first application's~~ proprietary identifier extension and resource identifier of said first firewall control block to said ~~second application's~~ proprietary identifier extension and resource identifier of said second firewall control block; and

allowing said first application to access said second application when said determining determines that access should be allowed.